Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application. These amendments are made without prejudice and solely to expedite prosecution of this application and shall not be taken as agreement with any position taken by the Examimer.

Listing of Claims:

1. (CURRENTLY AMENDED): The ~~A~~ method of claim 29 wherein said responding further comprises emulating a network of two or more distinct types of logic systems by a method comprising:

providing a plurality of actual logic systems of at least two distinct types;

providing a communication channel to said actual logic systems; and

running logic instructions on said actual logic systems whereby two or more said actual logic systems respond on said communication channel as though each were multiple logic systems, wherein an actual logic system responds as though it were multiple logic systems similar to its type.

2. (ORIGINAL): The method according to claim 1 further comprising:

at at least one of said actual logic systems, responding to multiple incoming addresses on said communication channel as though said at least one logic system were multiple logic systems.

3. (ORIGINAL): The method according to claim 1 further comprising:

on at least one actual logic system, providing varying responses.

4. (ORIGINAL): The method according to claim 3 wherein said responses vary based on an incoming address.

5. (ORIGINAL): The method according to claim 3 wherein said varying responses comprise varying time and use characteristics.

6. (ORIGINAL): The method according to claim 1 wherein said responses of said two or more actual logic systems are altered over time to emulate characteristics of real networks.

7. (ORIGINAL): The method according to claim 1 wherein said emulation is used to deceive unauthorized users trying to access one or more protected logic systems.

8. (ORIGINAL): The method according to claim 7 wherein said emulation is used to deceive unauthorized users trying to access one or more protected logic systems by providing deceptive responses to unauthorized datagrams so as to lead an unauthorized user to believe the user has accessed an actual computer system.

9. (ORIGINAL): The method according to claim 1 wherein said emulation is controllable from one or more control systems.

10. (ORIGINAL): The method according to claim 9 wherein said one or more control systems comprise one or more distributed control systems.

11. (ORIGINAL): The method according to claim 1 wherein said distinct types comprise different operating systems.

12. (ORIGINAL): The method according to claim 1 wherein said distinct types comprise:
different operating systems; and
different hardware platforms.

13. (CURRENTLY AMENDED): A computer network deception ~~emulation~~ system comprising:
two or more emulation computer systems for providing deceptions of at least two distinct types;
a network able to deliver datagrams to said two or more emulation computer systems; and
wherein two or more of said two or more emulation computer systems provides ~~emulation~~ deception responses of multiple emulated computer systems at multiple addresses, each emulation computer system providing deception ~~emulation~~ responses of emulated computers appropriate to said emulation computer system's type.

14. (ORIGINAL): The system according to claim 13 further comprising:

a transmission control system able to establish and vary delivery paths to said emulation computer systems.

15. (ORIGINAL): The system according to claim 13 further comprising:

an emulation control system able to establish and vary emulations provided by said two or more emulation computer systems.

16. (CURRENTLY AMENDED): A method of providing deception at a computer system by connecting an emulation subnetwork to a network through an emulation wall comprising:

receiving a datagram at an outside of an emulation wall;

determining that said datagram should be handled in said emulation subnetwork;

translating an original address indication of said datagram into a proxy address indication;

passing said datagram into said emulation subnetwork while translating said proxy address into an emulation original address indication; and

routing said packet in said emulation subnetwork based on said emulation original address indication.

17. (ORIGINAL): The method according to claim 16 further comprising:

receiving a response at an inside of said emulation wall from said emulation subnetwork;

translating a response emulation original address indication to a response proxy address indication; and

passing said datagram into said network from said emulation subnetwork while translating said response proxy address indication back to a response original address indication.

18. (ORIGINAL): The method according to claim 16 wherein address indications comprise source and destination addresses according to a standard networking protocol.

19. (ORIGINAL): The method according to claim 18 wherein address indications comprise source and destination addresses according to an IP networking protocol.

20. (ORIGINAL): The method according to claim 16 wherein said emulation original address indication is identical to said original address indication.

21. (ORIGINAL): The method according to claim 16 wherein said passing comprises:

receiving said datagram at a first standard network gateway;

translating said original address indication of said datagram into a proxy address indication at said first standard network gateway using a standard translation procedure;

routing said datagram with said proxy address indication to a second standard network gateway;

translating said proxy address indication of said datagram into said emulation original address indication at said second standard network gateway using a standard translation procedure; and

forwarding said datagram with said emulation original address indication to said emulation subnetwork.

22. (CURRENTLY AMENDED): ~~An~~ A deception emulation wall connecting ~~an emulation~~ a deception subnetwork to an outside network comprising:

an outside layer able to detect datagrams in said outside network to be handled in said ~~emulation~~ deception subnetwork;

a transport module, able to transport said datagrams into an internal ~~emulation~~ deception network while preserving their original source and destination address;

one or more emulation systems on said ~~emulation~~ deception subnetwork able to receive said datagrams with original source and destination address and to generate appropriate response datagrams onto said ~~emulation~~ deception subnetwork; and

an inside layer able to detect response datagrams to be transferred to said outside network; said transport facility able to transport said datagrams to said outside network.

23. (ORIGINAL): The device according to claim 22 wherein said outside layer and said inside layer are two network interfaces in a specialized network translation device and said transport module is implemented in specialized datagram handling logic in said device:

24. (ORIGINAL): The device according to claim 22 wherein:

said outside layer comprises an outside interface of a first standard network address translation module;

and said inside layer comprises an inside interface of a second standard network address translation module;

said transport module is implemented by performing a first translation within said first standard network address translation module into a proxy address, communicating a translated datagram to said second standard network address translation module and translating from the proxy address back to the original address on said emulation subnetwork.

25. (CURRENTLY AMENDED): The ~~A~~ method of claim 29 further wherein said deception is used for countering attacks in a network and further comprising:

at an emulation computer system in said network, accepting network protocol datagrams that are unauthorized; and

responding, by said computer system, to unauthorized datagrams using different emulations so that an attacker perceives that a number of different computer systems within said network have been reached.

26. (ORIGINAL): The method according to claim 25 wherein a network protocol datagram is detected as unauthorized by detecting that said datagram is addressed to a computer system that does not actually exist on said network.

27. (CURRENTLY AMENDED): The method according to claim 25 further comprising:

at a normal computer in said network, detecting unauthorized network protocol datagrams addressed to said normal computer; and

routing said unauthorized network protocol datagrams addressed to said normal computer to ~~said~~ an emulation computer using an address translation, for response by said emulation computer.

28. (ORIGINAL): The method according to claim 25 wherein an apparent emulated architecture changes with time or incoming viewpoint just as a large scale computer network changes with time and viewpoint.

29. (ORIGINAL): A method of providing deception at a computer system on a network comprising:

accepting, at said computer system, network protocol datagrams addressed to different computers; and

responding, by said computer system, to received datagrams using different deception emulations so that a receiver perceives that a number of different computer systems have been reached.

30. (ORIGINAL): A method of protecting a computer network against unwanted attacks comprising:

routing datagrams addressed to non-existing computers to a deception system; and

at said deception system, responding to said datagrams using varying emulations.

31. (ORIGINAL): The method according to claim 30 wherein said emulations vary based on one or more parameters including datagram addresses, time, or usage statistics.

32. (ORIGINAL): The method according to claim 30 wherein an emulation at a particular IP address translates the same services differently for different remote access points, creating for some, the illusion of a first network, for others the illusion of a service system with a vulnerable deception target, and for still others, access to other systems.

33 to 73 CANCELLED